National Security Agency/Central Security Service

INFORMATION ASSURANCE DIRECTORATE

CRITERIA FOR COMMERCIAL SOLUTIONS FOR CLASSIFIED (CSFC) SOLUTION INTEGRATORS

These criteria and processes are defined to provide a common baseline for CSfC solution integrators, enabling NSA, Authorizing Officials (AOs), and Designated Approving Authorities (DAAs) to assess the capabilities of solution integrators and accept their results.

Commercial Solutions for Classified Program Management Office (CSfC PMO)
V 1.0(U) (U) / 19 Sep 2013

Contents

Introduction

NSA's Commercial Solutions for Classified Program Management Office (CSfC PMO) provides the following criteria to establish a baseline for CSfC integrators. Integrators who demonstrate compliance to these criteria and sign a Memorandum of Agreement (MoA) with NSA have the option to be listed as CSfC Integrators on www.nsa.gov.

A CSfC Integrator is defined as an organization that meets the following criteria and is qualified to assemble and integrate components according to a CSfC Capability Package (CP), test the resulting solution, and provide a body of evidence to the solution Authorizing Official (AO)/Designated Approving Authority (DAA).

To perform these tasks, the organization shall have demonstrated experience in system integration, with the technologies to be integrated, in formal testing processes, and in evidence generation for system authorization.

1. Criteria for CSfC Integrators

These criteria cover two areas, organizational criteria and personnel criteria.

1.1. Organization

The organization shall meet the requirements of International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 17025:2005, "General requirements for the competence of testing and calibration laboratories" or be approved under the National Voluntary Lab Accreditation Program according to NIST Handbook 150.

NSA will assess whether organizations meet the criteria for CSfC Integrators. NSA may periodically have the integrators' processes and facilities inspected to ensure the criteria continue to be met.

1.1.1. Additional Management Requirements

a) The organization shall ensure that objective personnel are used to test the integrated system – separate from the personnel who assemble and configure the system.

b) The management system shall include policies and procedures to ensure the protection of information. Only persons authorized to work on a particular integration activity shall have access to related information.

c) The integrator shall maintain a record-keeping system that is used to track each effort. Records shall be complete with enough data to allow an independent body to review and concur with the work performed.

d) All solution integration efforts shall follow a current National Security Agency (NSA)/Information Assurance Directorate (IAD) approved Capability Package (CP).

1.1.2. Access to Secure Facility

It is not required that the integrator have a secure facility. However, the integrator must have access to a secure facility where they can receive classified risk assessments and test for classified vulnerabilities if needed. The facility clearance shall be equivalent to the level of data to be processed by the solution.

1.1.3. Reporting Requirements

a) Organizations seeking recognition as a CSfC Integrator shall provide documented evidence of compliance to the NSA/IAD.

b) Organizations shall submit Internal Audit documentation to NSA/IAD at least annually.

1.1.4. Test Methodology

The organization shall maintain standards and guidelines for methodologies to perform each of the following types of testing. The Capability Package provides guidelines for the development of a Test & Evaluation (T&E) Plan and Procedures. Phases of testing shall include the following.

a) Integration Testing – Integration testing shall focus on the flow of data between CSfC solution components.

b) System Testing – System testing shall test all requirements in the Capability Package on a documented end to end commercial solution.

c) Security Testing – Security testing shall verify all security requirements.

d) Penetration Testing – Penetration testing shall validate how the system functions when presented with unexpected input, i.e., fuzz testing. The sufficiency of penetration testing should be agreed to by the integrator and the customer.

1.1.5 Memorandum of Agreement

Upon being successfully vetted as a CSfC integrator, the organization will enter into a Memorandum of Agreement (MoA) with NSA.

1.2. Personnel

The integrator shall employ managerial and technical personnel to fulfill a number of roles per ISO/IEC 17025. Specific to the focus of this work, personnel performing, supervising, auditing, or providing quality control of these efforts shall hold at least one of the following certifications in the appropriate column.

IAT Level I	IAT Level II	IAT Level III
A+ CE	GIAC Security Essentials (GSEC)	CISA (with hands-on experience)
Network+ CE	Security+ CE	CISSP (with hands-on experience)
SSCP (with hands-on experience)	SSCP (with hands-on experience)	CASP
		GIAC Certified Incident Handler (GCIH) (with IAT Level II)
		GIAC Certified Enterprise Defender (GCED)

Table 1: Department of Defense (DoD) Approved Baseline Certifications (modified)

1.2.1. Capability Assembly and Configuration

The role of the capability assembly and configuration personnel is to select and procure CSfC components.

All personnel assigned to assemble and configure the solutions shall be knowledgeable in computing and network environments. They shall comply with the Information Assurance Technical (IAT) Level II criteria which require at least one of the certifications indicated in Table 1. Additionally, the individuals assembling and configuring the solutions should have certifications in the components being integrated. For example, if the solution includes Cisco products, integrating personnel should be Cisco certified. If the solution includes Microsoft products, the integrators should be Microsoft certified. Updated certification requirements can be found at iase.disa.mil.

1.2.2. Capability Testing

All testing personnel shall be IAT Level III and shall have additional experience/training in the devices being integrated.

Personnel shall have experience in the required component and system testing.

1.2.3. Capability Documentation

Technical writers and editors shall be employed to produce complete documentation of the effort.

Documentation to be prepared shall include, but is not limited to:

a) Solution components and configuration baseline

b) Certificate Policy (CP)/Certification Practice Statement (CPS)

c) Test Plan and Test Procedures, per guidance provided in the Capability Package

d) Final Test Report to include security and non-security discrepancies

e) Other documentation as required by the AO/DAA

1.2.4. Personnel Clearances

Integrator personnel shall hold clearances that enable them to receive risk assessments and adequately address vulnerabilities: Clearances shall be equivalent to the level of data to be processed by the solution.

2. CSfC Integrator Application: Required Information

The following application shall be provided to CSfC@nsa.gov to demonstrate compliance with these requirements:

1. Legal name and full address of the integrator:
2. Ownership of the integrator:
3. Authorized representative's name and contact information:
4. Does your organization meet ISO/IEC 17025:2005? Y/N
5. Is your organization approved under the National Voluntary Lab Accreditation Program? Y/N
6. Facility clearance level for your organization:
7. Titles, certification, and clearance information for personnel filling key roles identified in the criteria:

Title	Certifications	Clearance

8. Please cite your organization's relevant prior experience, to include technologies, capability packages, component and system testing:
9. Please cite previous customers who have employed your integrator expertise: